View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Southern Methodist University

Science and Technology Law Review

Volume 18 | Number 4 Article 4

2015

The Impact of HIPAA (and Other Federal Law) on Wearable Technology

Timothy Newman

Jennifer Kreick

Follow this and additional works at: https://scholar.smu.edu/scitech

Recommended Citation

Timothy Newman et al., *The Impact of HIPAA (and Other Federal Law) on Wearable Technology*, 18 SMU Sci. & Tech. L. Rev. 429 (2015)
https://scholar.smu.edu/scitech/vol18/iss4/4

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.

The Impact of HIPAA (and Other Federal Law) on Wearable Technology

*Timothy Newman**
*Jennifer Kreick***

It can track the number of steps you take, and it can track your heart rate. It can tell you how active you were today, how many stairs you climbed, and how many calories you have burned. It can even tell you how soundly you slept last night. And all of this information can be stored on a smart device application or "app." "It" is wearable technology. Wearable technology can track and retain much information to help ordinary people take charge of their health.

But what happens when the information that this technology collects is shared with health care providers? Do our devices now have to comply with the U.S. Health Insurance Portability and Accountability Act (HIPAA)? What federal agencies' enforcement activities may impact the way wearable technology stores and shares health information? This article explores the impact of HIPAA and other federal regulations on the health information that wearable technology and other mobile applications store and transmit and when exactly the sharing of that data and the device itself are subject to regulation.[1]

I. WEARABLE TECHNOLOGY

Wearable technology comes in all shapes and sizes. Users can wear it on their wrists, clip it to their belts, carry it in their pockets, or download it to a mobile device. Manufacturers shipped more than eighteen million wearable technology devices in the second quarter of 2015.[2] More than four million of

---

* Timothy Newman is an attorney at Haynes and Boone, LLP in Dallas, Texas. He speaks and writes regularly on topics related to cybersecurity.

** Jennifer Kreick is an attorney at Haynes and Boone, LLP in Dallas, Texas. She speaks and writes regularly on topics related to cybersecurity.

1. This article does not address all federal laws and regulations potentially applicable to wearable technology such as medical device regulations and guidance issued by the Food and Drug Administration or health claims regulated by the Federal Trade Commission. In addition to federal laws and regulations, states often regulate the privacy and security of health information. For example, the Texas Medical Records Privacy Act applies to any person who comes into possession of protected health information. *See* TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2)(B) (West 2015). The statute sets forth specific requirements regarding employee training, electronic disclosures, marketing, and sale of protected health information.

2. *See* Andrew Nusca, *The Numbers Are in: Apple is No. 2 in Wearables*, FORTUNE (Aug. 27, 2015, 10:40 AM), http://fortune.com/2015/08/27/apple-wearables-market-share.

those devices were the popular Fitbit,[3] a device manufactured by Fitbit, Inc. that can track a user's steps, heart rate, and distance walked.[4] Fitbit can also track the number of stairs the user has climbed, report the user's active minutes throughout the day, and provide information about how soundly the user slept through the night.[5]

Apple, Inc. recently joined the fray, shipping more than 3.6 million smart watches in the second quarter of 2015.[6] The Apple Watch can track a user's steps and calories burned, and it can track how many times a user stands up throughout the day.[7] The Mi Band by Xiaomi Inc., which garnered seventeen percent of the market in the second quarter of 2015,[8] can monitor a user's sleep patterns and provide action plans for improving sleep.[9] Most devices allow users to retain their information and incorporate goals into their technology, helping users become more aware of their activity and allowing them to monitor their exercise.

With all this novel technology, consumers expect wearable technology to improve continually. And one should not underestimate the potential for sharing the information that these devices collect. For example, if primary care providers used information that their patients' wearable technology tracked, they could more effectively monitor their patients' health and recommend more appropriate treatment programs. Employers could stay more in sync with their work force's health in order to provide incentives or resources to help their employees maintain their health. Still more, health insurers could more effectively assess risk in their insured population. Researchers could use the devices to keep tabs on participants in clinical trials. In other words, the possibilities are limitless.

But storing and sharing information shifts the conversation about wearable devices and mobile health applications. Wearable technology is no longer simply a tool for users to monitor their health and wellness more effectively. Instead, the technology is likely subject to more intense scrutiny and complex regulation and could potentially create liability for developers.

The marketplace has taken note of the concerns regarding health data, information sharing, and privacy. For example, in 2014, Apple implemented privacy protections for the health data created and stored on the smartwatch,

3. *See id.*

4. *See Shop the Store*, Products, FITBIT, https://www.fitbit.com/store?gclid=CIunstqb8MgCFRAvaQodi18Brg (last visited May 10, 2016).

5. *See id.*

6. *See* Nusca, *supra* note 2.

7. *See Watch*, Health and Fitness, APPLE, http://www.apple.com/watch/health-and-fitness/ (last visited May 10, 2016).

8. *See* Nusca, *supra* note 2.

9. *See Mi Band*, Features, XIAOMI, http://www.mi.com/en/miband/#01 (last visited May 10, 2016).

including a requirement that users give consent before application developers can gain access to users' health information, encryption of the data stored on the smartwatch, and assurances to the U.S. Federal Trade Commission (FTC) that the health data would not be sold to third-party marketers.[10] Recently, Fitbit announced that it would support HIPAA compliance in an effort to allow the lawful sharing of information from its devices.[11] Yet, questions remain for many companies regarding what regulations apply to these wearable devices when they store and transmit health information, and how to properly address these regulations. Unfortunately, the answers to many of these questions are not always straightforward.

II. HIPAA: WHEN AND HOW IT APPLIES

In 1996, Congress passed HIPAA, which includes numerous provisions relating to various aspects of the health care system.[12] HIPAA regulations incorporate privacy and security protections for individually identifiable health information.[13] The United States Department of Health and Human Services (HHS) publishes the HIPAA regulations relevant to the privacy and security of health information.

The regulations are divided into several parts, with the Privacy Rule and the Security Rule being the most relevant to this article. The Privacy Rule can be found in the Code of Federal Regulations in 45 C.F.R. Part 160 and Subparts A and E of Part 164.[14] HHS published the final Privacy Rule in December 2000[15] and modified the rule in August 2002.[16] HHS required compliance with the Privacy Rule as of April 14, 2003 (April 14, 2004 for small health plans).[17] The Security Rule is located in 45 C.F.R. Part 160 and

10. *See* Christina Farr & Diane Bartz, *Exclusive: U.S. FTC Asking Apple About Health Data Protection*, REUTERS (Nov. 13, 2014, 4:29 PM), http://www.reuters.com/article/2014/11/13/us-apple-ftc-exclusive-idUSKCN0IX2I520141113#TdWpbhh04GUzMPOP.97.

11. *See* Press Release, Victoria Gavaza, Fitbit, Inc. (Sept. 16, 2015), https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx.

12. *HIPAA Administrative Simplification Statute and Rules*, U.S. DEP'T. OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/ (last visited May 10, 2016).

13. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 100 Stat. 2548.

14. 45 C.F.R. §§ 160.101, 164.104 (2016).

15. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000) (codified at 45 C.F.R. §§ 160, 164), http://www.hhs.gov/sites/default/files/introduction.pdf.

16. *Id.* at 65 Fed. Reg. 53182 (Aug. 14, 2002) (codified at 45 C.F.R. §§ 160, 164), http://www.hhs.gov/sites/default/files/introduction.pdf.

17. *Id.*

Subparts A and C of Part 164.[18] HHS published the final Security Rule in February 2003.[19] HHS required compliance with the Security Rule as of April 21, 2005 (April 21, 2006 for small health plans).[20]

In 2009, President Barack Obama signed into law the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009.[21] Although HITECH was enacted to promote the adoption and meaningful use of health information technology, concerns regarding the privacy and security of electronic health information prompted HHS to strengthen certain HIPAA privacy, security, and enforcement provisions as well.[22] In January 2013, HHS published its final rule, known as the "Omnibus Rule," implementing provisions of the HITECH Act.[23]

In general, the Privacy Rule requires certain entities (including health plans, health care clearinghouses, and health care providers that conduct certain health care transactions electronically) to protect the privacy of individuals by establishing certain safeguards and imposing limitations on disclosures of individually identifiable health information.[24] The Privacy Rule also grants individuals certain rights over their health information such as allowing them to obtain a copy of their medical records.[25] While the Privacy Rule applies broadly to individually identifiable health information in any form (i.e., paper, electronic, or oral), the Security Rule applies specifically to electronic protected health information.[26] The Security Rule establishes administrative, physical, and technical safeguards to protect this electronic health informa-

18. 45 C.F.R. §§ 160.103, 164.306.

19. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (codified at C.F.R. §§ 160, 162, 164), https://www.gpo.gov/fdsys/granule/FR-2003-02-20/03-3877.

20. *Id.*

21. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115. (codified at 42 U.S.C. § 17938).

22. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at C.F.R. §§ 160, 164), http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

23. *Id.*

24. 65 Fed. Reg. 53182 (codified at 45 C.F.R. §§ 160, 164), https://www.gpo.gov/fdsys/pkg/FR-2002-08-14/pdf/02-20554.pdf.

25. *Id.*

26. *See id.*; 68 Fed. Reg. 8334 (codified at C.F.R. §§ 160, 162, 164), https://www.gpo.gov/fdsys/granule/FR-2003-02-20/03-3877.

tion.[27] HHS's Office of Civil Rights (OCR) enforces the Privacy Rule and the Security Rule.[28]

A. Key Definitions: Covered Entity, Business Associate, and Protected Health Information

HIPAA applies only to covered entities and their business associates.[29] Accordingly, if an entity fails to meet the definition of a covered entity or business associate, the entity does not need to comply with HIPAA.[30] "Covered entities" include health plans, healthcare clearinghouses, and health care providers that conduct certain transactions electronically, such as submitting claims to health plans electronically.[31] For example, doctors, clinics, psychologists, dentists, nursing homes, and pharmacies are considered covered entities if they transmit any information in electronic form in connection with a transaction for which HHS has adopted a standard.[32] Likewise, a health insurance company or a government program that pays for health care, such as Medicare and Medicaid, is a covered entity.[33]

A "business associate" is an entity that performs certain functions or activities that involve the use or disclosure of "protected health information" on behalf of, or provides certain services to, a covered entity that is not a member of the covered entity's workforce.[34] The Privacy Rule identifies some functions, activities, and particular services that render an individual or entity a business associate, if the activity or service involves the use or disclosure of protected health information.[35] Specifically, these activities include when "a business associate . . . (i) on behalf of [the] covered entity . . . , creates, receives, maintains, or transmits protected health information for a function or activity regulated" by HIPAA such as payment or health care operations activities, "including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities . . . , billing, benefit management, practice management, and repricing"; or (ii) provides "legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or

27. 68 Fed. Reg. 8334 (codified at C.F.R. §§ 160, 162, 164), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

28. *How OCR Enforces the HIPAA Privacy & Security Rules*, U.S. DEP'T. OF HEATH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html (last visited May 10, 2016).

29. 45 C.F.R. § 160.102.

30. *Id.*

31. *Id.* § 160.103.

32. *See id.*

33. *See id.*

34. *Id.*

35. *Id.*

financial services to or for a covered entity . . . where the provision of the service involves the disclosure of protected health information . . . ."[36] For instance, a business associate includes law firms or accounting firms whose services to a health care provider involve access to protected health information.[37] Similarly, a third party administrator that assists a health plan with claims processing or a data hosting company that stores protected health information on behalf of a health care provider would likely qualify as a business associate.[38] A covered entity can be a business associate of another covered entity, and subcontractors of a business associate or covered entity can also qualify as business associates.[39]

HIPAA provides safeguards for "protected health information" that is held or transmitted by a covered entity or its business associate.[40] Protected health information is information that identifies an individual (or for which there is a reasonable basis to believe it can be used to identify the individual) and relates to the individual's physical or mental health, the provision of health care services to the individual, or payment for such health care services.[41] Protected health information includes information maintained in any form, such as paper, electronic, or oral.[42] Thus, protected health information would include certain demographic information such as name, address, date of birth, or social security number, if it can be associated with health information (such as the individual's mental or physical health or the payment for health care services). For example, a laboratory report, hospital bill, or a patient's medical record would likely be protected health information if it is held by a covered entity or business associate.

A covered entity or business associate may avoid HIPAA's application by creating information that is not individually identifiable, or de-identifying information based on requirements outlined under the Privacy Rule.[43] Thus, the covered entity or business associate can use and disclose the de-identified information because it does not identify the individual, and there is no reasonable basis to believe it could be used to identify the individual.[44]

The Privacy Rule provides two de-identification methods. The first involves a formal determination by a qualified expert.[45] The second involves

36. *Id.*

37. *See* 45 C.F.R. § 160.103.

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.*

42. *Id.*

43. 45 C.F.R. § 164.514 (a)–(b) (2013).

44. *See id.* § 164.514(b)(1).

45. *See id.*

the removal of eighteen individual identifiers, as well as the absence of actual knowledge that the remaining information could be used, alone or in combination with other information, to identify the individual.[46] The eighteen identifiers that must be removed include:

(1) Names;
(2) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
    (i) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
    (ii) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000;
(3) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(4) Telephone numbers;
(5) Fax numbers;
(6) Email addresses;
(7) Social security numbers;
(8) Medical record numbers;
(9) Health plan beneficiary numbers;
(10) Account numbers;
(11) Certificate/license numbers;
(12) Vehicle identifiers and serial numbers, including license plate numbers;
(13) Device identifiers and serial numbers;
(14) Web Universal Resource Locators (URLs);
(15) Internet Protocol (IP) addresses;
(16) Biometric identifiers, including finger and voice prints;
(17) Full-face photographs and any comparable images;
(18) Any other unique identifying number, characteristic, or code.[47]

A covered entity, however may assign a code or other means of record identification to allow re-identification, provided that:

46. *See id.* § 164.514(b)(2).

47. *See id.*

(i) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
(ii) Security. The covered entity does not use or disclose the code or other means of record identification is not used or disclosed for any other purpose, and does not disclose the mechanism for re-identification.[48]

Because the requirements for de-identifying protected health information are fairly strict, health information that may appear at first glance not to be individually identifiable (e.g., patient initials and date of service) could still constitute protected health information under HIPAA.

B. Requirements for Sharing Information with Business Associates

The Privacy Rule applies certain limitations to the use and disclosure of protected health information by covered entities. For example, a covered entity is generally not allowed to disclose protected health information to a third party without an individual's authorization.[49] However, a covered entity is permitted to disclose protected health information to a business associate for certain purposes if the covered entity obtains "satisfactory assurances" that the business associate will apply certain protections to the information.[50] The satisfactory assurances must be a written contract, agreement, or arrangement that incorporates a specific list of elements, known as a "business associate agreement."[51] The required elements for all business associate agreements can be found in the federal register at section 164.504(e)(2).[52] HHS has published a sample business associate contract that includes the required elements.[53]

There are certain exceptions to the requirement that a business associate agreement be in place prior to the use or disclosure of protected health information. For example, disclosures by a covered entity to a health care provider for the treatment of an individual do not require business associate

48. *See id.* § 164.514(c).

49. *See* 45 C.F.R. § 164.502(a) (2016).

50. *See id.* § 164.502(e)(1).

51. *See id.* § 164.502(e)(2).

52. *Id.*

53. *Id.* The 2013 Omnibus Rule modified some of the required elements. For example, the Omnibus Rule added a new required provision: "To the extent the business associate is to carry out a covered entity's obligation under this subpart, [the business associate must] comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation." *See* 45 C.F.R. § 164.502(e)(2).

agreements.[54] Thus, a physician need not have a business associate agreement with a laboratory in order to disclose protected health information for treatment of the patient.[55] There are other exceptions as well, including one for persons or organizations whose services do not involve the use or disclosure of protected health information and where any access to protected health information by such persons would be incidental, if at all (i.e., a janitorial service or electrician).[56] Further, persons or organizations that act merely as a conduit for protected health information are excepted, such as the U.S. Postal Service, certain private couriers, and their electronic equivalents.[57]

The 2013 Omnibus Rule included several key regulatory changes for business associates. Prior to the Omnibus Rule, for example, business associates had a contractual obligation to comply with the Security Rule because covered entities were required to have a business associate agreement in place, and the covered entities were required to include certain provisions in the business associate agreement.[58] Thus, in effect, business associates were required by their contracts with the covered entities to comply with certain provisions of the Privacy Rule and Security Rule.[59]

With the Omnibus Rule, HHS clarified that business associates are directly liable for violating the Security Rule and certain provisions of the Privacy Rule.[60] Thus, OCR may now enforce civil monetary penalties against not only covered entities, but also against business associates.[61] Under the Omnibus Rule, business associates are now directly liable for: (i) compliance with the Security Rule;[62] (ii) impermissible uses and disclosures of protected health information;[63] (iii) failure to provide breach notification to the covered entity;[64] (iv) failure to provide access to a copy of electronic protected health information as necessary to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of protected health informa-

54. *Id.* § 164.502(e); *see also Health Information Privacy: Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.

55. 45 C.F.R. § 164.502(e).

56. *Id.*

57. *Id.*

58. Peggy L. Barlett et al., *HIPAA Omnibus Final Rule Has Important Changes for Business Associates and Covered Entities*, GODFREY KAHN S.C., http://www.gklaw.com/news.cfm?action=pub_detail&publication_id=1270 (Mar. 25, 2013).

59. *See id.*

60. *Id.*

61. *Id.*

62. *How OCR Enforces the HIPPA Privacy & Security Rules*, *supra* note 28.

63. 45 C.F.R. § 164.502(a)(3); *id.*

64. 45 C.F.R. § 164.410.

tion;[65] (v) failure to disclose protected health information to the Secretary of HHS when required to investigate or determine the business associate's compliance with HIPAA;[66] (vi) failure to provide an accounting of disclosures when required;[67] (vii) failure to comply with the minimum necessary standards;[68] and (viii) failure to enter into business associate agreements with subcontractors that create or receive protected health information.[69]

C. HIPAA Breaches and Security Rules

In general, HIPAA requires business associates and covered entities to provide notifications regarding breaches of unsecured (i.e., unencrypted) protected health information. A "breach" is defined as the acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information in a manner not permitted under the Privacy Rule.[70] "Unsecured" protected health information refers to protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the HHS Secretary in HHS guidance (i.e., the information was encrypted if electronic or shredded if in paper form).[71] The term "breach" excludes

> [a)] Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule;
> [b)] Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or
> [c)] A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unau-

65. *Id.* § 164.502(a)(4)(ii).

66. *Id.* § 164.502(a)(4)(i).

67. 76 Fed. Reg. 31426 (May 31, 2011).

68. 45 C.F.R. § 164.502(b).

69. *Id.* § 164.502(e)(1)(ii).

70. *Id.* § 164.402.

71. *Id.*

> thorized person to whom the disclosure was made would not reasonably have been able to retain such information.[72]

The reporting obligations under HIPAA for covered entities and business associates differ. While a business associate is required to report the breach only to the covered entity involved, the covered entity is required to report to the individuals impacted by the breach, to HHS, and potentially to the media or on its website.[73] Although HIPAA does not require the business associate to notify individuals or HHS in the event of a breach, the covered entity may pass these reporting obligations down to the business associate, such as by delegating the reporting obligations in a business associate agreement.

A breach of unsecured protected health information is treated as "discovered" by the covered entity or business associate as of the first day on which such breach is known to the covered entity or business associate, "or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity or business associate (determined in accordance with the federal common law of agency)."[74]

The 2013 HIPAA regulations included certain significant revisions to the Breach Notification Rule. For example, they added a provision stating that an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

> a) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
> b) The unauthorized person who used the protected health information or to whom the disclosure was made;
> c) Whether the protected health information was actually acquired or viewed; and
> d) The extent to which the risk to the protected health information has been mitigated.[75]

This new standard replaced the previous standard that was largely based on the potential harm to individuals resulting from a breach.

Covered entities suffering a breach must notify affected individuals without unreasonable delay and in no case later than 60 days following dis-

72. *Id.*

73. *Id.* § 164.410, § 164.404–08.

74. 45 C.F.R. § 164.410(a)(2).

75. *Id.*

covery.[76] For breaches involving less than 500 individuals, the covered entity must also notify the HHS Secretary via the HHS website on an annual basis no later than 60 days after the end of the calendar year in which the breach was discovered.[77] For breaches involving 500 or more individuals, the covered entity must notify the HHS secretary via the HHS website contemporaneous with the individual notices and if the breach of unsecured protected health information involves more than 500 residents of a state or jurisdiction, notify prominent media outlets serving the state or jurisdiction without unreasonable delay and in no case later than 60 days after discovery of the breach.[78]

The individual notifications must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach (such as full name, social security number, date of birth, home address, diagnosis code, etc.), the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.[79]

Note that if individual notification is required, the covered entity must notify affected individuals in written form by first class mail, or by email if the individual has agreed to receive such notices electronically.[80] If the covered entity has insufficient contact information for 10 or more individuals, the covered entity must provide substitute individual notice either by posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

In addition to reporting breaches under the Breach Notification Rule, the Security Rule requires all business associates and covered entities to implement policies and procedures to address security incidents.[81] The term "security incident" is defined broadly to include the attempted or successful

76. *Id.* § 164.404. There is an exception to all of the timing requirements for law enforcement delay.

77. *Id.* § 160.408(c).

78. *Id.* § 164.408(b), § 164.406.

79. *Id.* § 164.404.

80. 45 C.F.R. § 164.404(d)(2).

81. *Id.* § 164.308(a)(6)(i).

unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.[82]

All business associates and covered entities must "identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes."[83] HIPAA also requires covered entities and business associates to include in their business associate agreements a provision requiring business associates to report to the covered entities any security incident of which the business associate becomes aware, including breaches of unsecured health information as required by the Breach Notification Rule.[84] Unlike the Breach Notification Rule, there is no specific time period during which a security incident that does not rise to the level of a breach must be reported.

HHS has issued guidance on its website regarding how to comply with the HIPAA requirements for addressing security incidents. Specifically, HHS said:

> In addressing the Security Incident Procedures standard [at 45 C.F.R. § 164.308(a)(6)(i)], a covered entity may consider some of the following questions: what specific actions would be considered security incidents; how will incidents be documented and reported; what information should be contained in the documentation; how often and to whom should incidents be reported; what are the appropriate responses to certain incidents; and whether identifying patterns of attempted security incidents is reasonable and appropriate. When taking into consideration the requirements of § 164.306(a) and (b), and its risk analysis, the covered entity may decide that certain types of attempted or successful security incidents or patterns of attempted or successful incidents warrant different actions.
>
> For example, a covered entity may decide that a "ping" (a request-response utility used to determine whether a specific Internet Protocol (IP) address, or host, exists or is accessible) on the communications network initiated from an external source would require the following actions to comply with the standard; (1) minimal, if any, response; (2) no mitigation actions since no harmful effects were caused by the incident; and (3) brief documentation of the security incident and outcome, such as, a recording of aggregate statistical information. Based on its analysis, the entity may also determine that other types of incidents, such as suspicious patterns of "pings" on the communications network initiated from an ex-

82. *Id.* § 164.304.

83. *Id.* § 164.308(a)(6)(ii).

84. *Id.* § 164.314.

ternal source or a specific malicious security incident would require a more detailed response, mitigation steps, and more detailed documentation of the incident and outcome. While internal reporting of security incidents is an inherent part of security incident policies and procedures, the Security Rule generally does not require a covered entity to report incidents to outside entities. However, § 164.314(a)(2)(i)(C) and (b)(2)(iv) require contracts between a covered entity and a business associate, and plan documents of a group health plan, respectively, to include provisions that require business associates and plan sponsors to report to the covered entity any security incidents of which they become aware.[85]

D. Enforcement and Penalties

OCR enforces the Privacy Rule and Security Rule within the confines of HIPAA regulations.[86] Potential civil monetary penalties vary based on the violator's level of intent, as detailed in the chart below.[87]

Violation	Amount Per Violation	Limit for All Violations of an identical provision in a calendar year
Unknowing violation	$100 – $50,000	$1,500,000
Violation with reasonable cause to know	$1,000 – $50,000	$1,500,000
Willful neglect – corrected	$10,000 – $50,000	$1,500,000
Willful neglect – not corrected	$50,000	$1,500,000

In addition to civil penalties, OCR can refer matters involving willful neglect to the U.S. Department of Justice for potential criminal prosecution.[88] Both fines and criminal charges are generally reserved for more egregious cases, such as cases in which an entity fails to implement corrective actions

85. *Frequently Asked Questions*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2002.html.

86. *Health Information Privacy: HIPAA Enforcement*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/enforcement/ (last visited May 10, 2016).

87. *HIPAA Violations and Enforcement*, AM. MED. ASS'N, http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page? (last visited May 10, 2016).

88. *The Reality of HIPAA Violations and Enforcement*, HIPAA.COM, https://www.hipaa.com/the-reality-of-hipaa-violations-and-enforcement/.

or is uncooperative during an investigation.[89] OCR can issue fines for a multitude of HIPAA violations, including failure to conduct a risk assessment, failure to have adequate policies and procedures in place, or failure to secure information appropriately.[90] OCR can also initiate corrective action by regulated entities through a resolution agreement or otherwise. The corrective action plan may call for retraining staff on existing policies or revising policies and training of staff on the new policies.[91]

Technology often plays a role in HIPAA violations and subsequent fines. For example, in December 2014, OCR entered into a settlement with Anchorage Community Mental Health Services (ACMHS) for potential HIPAA violations.[92] Under the settlement agreement, ACMHS agreed to pay $150,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program.[93] The OCR investigation began after ACMHS reported a breach of unsecured electronic protected health information affecting 2,743 individuals when malware compromised the security of its information technology resources.[94] The OCR investigation revealed that although ACMHS had sample Security Rule policies and procedures, ACMHS did not follow the samples.[95] In addition, OCR alleged that

89. *Id.*

90. *Id.*

91. *See OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities*, U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE OF INSPECTOR GEN. (Sept. 2015), http://oig.hhs.gov/oei/reports/oei-09-10-00511.asp. In September 2015, the HHS Office of Inspector General (OIG) issued a report finding that OCR should strengthen its follow up of reported breaches of patient information. The report recommended that OCR (1) enter small-breach information into its case-tracking system or a searchable database linked to it; (2) maintain complete documentation of corrective action; (3) develop an efficient method in its case-tracking system to search for and track covered entities that reported prior breaches; (4) develop a policy requiring OCR staff to check whether covered entities reported prior breaches; and (5) continue to expand outreach and education efforts to covered entities. OCR responded to the report and concurred with these recommendations. With the recent focus on breaches involving unsecured protected health information and scrutiny on OCR to ensure consistent follow up regarding breaches, we will likely see continuing efforts to enforce the HIPAA rules, especially in small breaches (i.e., under 500 individuals) and in breaches where the covered entity has previously reported a breach. *Id.*

92. *Bulletin: HIPAA Settlement Underscores Vulnerability of Unpatched and Unsupported Software*, U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf (Dec. 2014).

93. *Id.*

94. *Id.*

95. *Id.*

ACMHS failed to identify and address basic risks, such as not regularly updating systems with available patches and running outdated, unsupported software.[96] In a statement, OCR Director Jocelyn Samuels said: "Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to [electronically protected health information] on a regular basis. This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks."[97]

In addition to the enforcement tools discussed above, HITECH requires HHS to perform periodic audits of covered entities and business associates to assess compliance with HIPAA.[98] In 2011, OCR established a pilot audit program to measure the efforts of 115 covered entities and developed an audit protocol.[99] OCR began phase two of its HIPAA audit program in March 2016.[100]

E. Recent HIPAA Developments in the Wearable Technology Industry

The mobile health industry has been active in requesting clarity and communication from HHS regarding HIPAA's impact on mobile health and wearable technology developers. In September 2014, ACT — The App Association wrote to U.S. Representative Tom Marino expressing concern about "a regulatory environment that has not kept pace with the rapid growth of technology that gives users greater access to healthcare providers and more control over their health information."[101] According to ACT, HHS needed to "take a fresh look at the implementation of [HIPAA] to ensure that it better fits today's mobile world."[102]

ACT made three specific suggestions for HHS.[103] First, ACT suggested that HHS should "make existing regulation more accessible for tech compa-

96. *Id.*

97. *Id.*

98. *HIPAA Privacy, Security, and Breach Notification Audit Program*, U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit (last visited May 10, 2016).

99. *Id.*

100. Press Release, U.S. Department of Health & Human Services, OCR Launches Phase 2 of HIPPA Audit Program (Mar. 21, 2016), *available at* http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html.

101. Letter from ACT — The App Ass'n to Rep. Tom Marino, U.S. House of Representatives (Sep. 15, 2014) (on file with author), *available at* http://actonline.org/wp-content/uploads/2014/10/HIPAA-Letter-to-Rep.-Marino.pdf.

102. *Id.*

103. *See id.*

nies" instead of relying on information "mired in a Washington, D.C. mindset that revolves around reading the *Federal Register*, or hiring expert consultants to 'explain' what should be clear in the regulation itself."[104] ACT also suggested that HHS "improve and update guidance from OCR on acceptable implementations" instead of "leaving app makers to learn about these through an audit."[105] Finally, ACT suggested that HHS "improve outreach to new entrants in the healthcare space" and "increase its participation in existing developer-focused events."[106]

Representative Marino and U.S. Representative Peter DeFazio relayed these concerns and requests to HHS Secretary Sylvia Burwell in September 2014.[107] In her response, Secretary Burwell highlighted HHS's efforts to provide more clarity around HIPAA requirements and more closely engage with mobile health developers.[108]

On October 5, 2015, likely in response to this exchange with industry leaders, OCR launched its new web platform for mobile health developers.[109] Although the platform is sparsely populated with content at this point, it allows individuals to interact with OCR by submitting questions and viewing responses.[110] This initiative provides some insight into OCR's education initiatives, and application developers' compliance frustrations. For example, one question and answer posted to the website reads as follows:

> Question: Developers need better guidance around patient generated health data, since HIPAA focusses [sic] on one-way data sharing from a provider/other covered entity outward to the patient/other entity. In the future, more and more data will be flowing in the opposite direction, and there should be guidance to clarify that HIPAA should not prevent the flow of information from the patient back to the provider.

104. *Id.*

105. *Id.*

106. *Id.*

107. Letter from Rep. Peter DeFazio and Rep. Tom Marino, U.S. House of Representatives, to Hon. Sylvia Mathews Burwell, Sec'y of Health & Human Servs., U.S. Dep't of Health & Human Servs. (Sep. 18, 2014) (on file with ACT — The App Association), http://actonline.org/wp-content/uploads/2014/09/Letter-to-Secretary-Burwell-September-18-2014.pdf.

108. Letter from Hon. Sylvia Mathews Burwell, Sec'y of Health & Human Servs., U.S. Dep't of Health & Human Servs., to Rep. Peter DeFazio, U.S. House of Representatives (Nov. 21, 2014) (on file with ACT — The App Association), http://actonline.org/wp-content/uploads/2015/01/HHS-Response-Letter-to-Defazio.pdf.

109. HIPAA QUESTIONS PORTAL, http://hipaaqsportal.hhs.gov/ (last visited May 10, 2016).

110. *See id.*

> Answer (from OCR): Information created or held by individuals/ patients/consumers is not subject to HIPAA unless and until it is received by a covered entity (or a business associate). HIPAA does not prevent hospitals, medical practices and other covered entities from receiving patient generated health data, whether by phone, paper, fax, online patient facing portal, or mHealth application. Note that under the HIPAA Security Rule, covered entities and business associates need to conduct a security risk analysis to evaluate and address the potential risks of any solutions deployed (e.g., web based portal, data transfer application, direct network connection, etc.) to receive and process ePHI from external sources.[111]

One can expect to see more manufacturers and developers taking advantage of this ability to confer with OCR.

In February 2016, OCR released additional guidance with specific scenarios to assist developers in determining whether HIPAA applies to them.[112] The guidance consists of a set of six specific scenarios, as well as certain questions that app developers should consider. OCR emphasized that the scenarios are highly dependent on the facts and circumstances, and even a slight change in facts could change the analysis.[113] For example, OCR stated that when a consumer downloads a health app to her smartphone and populates it with her own information (such as blood glucose levels and blood pressure readings she obtained herself using home health equipment), the app developer is not a business associate under HIPAA.[114] OCR made clear that the developer in this scenario is not creating, receiving, maintaining, or transmitting protected health information on behalf of a covered entity or business associate.[115]

Likewise, if a consumer uses a health app that is designed to help her manage a chronic condition and then adds her own information to the app (even if she downloads the data from her doctor's electronic health record through a patient portal and then uploads it into the app), the developer is still not a business associate since the consumer obtains the health information from her provider and then inputs it into the app for her own purposes.[116]

---

111. *Can HIPAA Address Patient Generated Data?*, HIPAA QUESTIONS PORTAL, http://hipaaqsportal.hhs.gov/a/dtd/Can-HIPAA-address-patient-generated-data/122277-36899 (last visited May 10, 2016).

112. *Health App Use Scenarios & HIPAA*, HIPPA QUESTIONS PORTAL, http://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/OCR-health-app-developer-scenarios-2-2016.pdf (last visited May 10, 2016).

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

OCR also stated that an app developer is not a business associate if a doctor recommends to her patient a particular app to track diet, exercise, and weight, and the patient downloads the app and uses it to send a summary report to her doctors before her next appointment.[117] The developer is not a business associate because the developer is not creating, receiving, maintaining or transmitting protected health information on behalf of a covered entity or business associate (note that the patient initiated the transmission to her physician).[118] Thus, although the doctor recommended the app, there is no indication that the doctors hired the developer to provide services to patients involving protected health information.[119]

OCR's guidance clarifies that a developer becomes a business associate only when the developer provides goods or services to or on behalf of a covered entity or business associate that involve the use or disclosure of protected health information. For example, OCR stated the following scenario would not render an app developer a business associate: (i) a consumer downloads a health app to her smartphone; (ii) the consumer requests that her health care provider and the app developer enter into an interoperability arrangement that allows for secure exchange of the consumer's information between the provider's electronic health record and the app; (iii) the consumer populates information on the app and directs the app to transmit the information to the provider; and (iv) the consumer is able to access her test results from the provider through the app.[120] In this scenario, the app developer is providing a service to the consumer at the consumer's request and is not using or disclosing protected health information on behalf of the covered entity.[121] "The app developer is transmitting data on behalf of the consumer to and from the provider."[122] The interoperability agreement alone is not enough to make the app developer a business associate of the provider since "the arrangement exists to facilitate access initiated by the consumer."[123]

In contrast, an app developer would be a business associate of a provider if the provider "has contracted with app developer for patient management services, including remote patient health counseling, monitoring of patients' food and exercise, patient messaging, EHR integration and application interfaces." The patient, at the direction of her provider, downloads the health app, and information the patient inputs is automatically incorporated into the provider's electronic health record.[124] In this scenario, the app devel-

117. *Id.*

118. *Health App Use Scenarios & HIPAA*, *supra* note 112.

119. *Id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. *Health App Use Scenarios & HIPAA*, *supra* note 112.

oper contracts with the provider for certain services that involve the use and disclosure of protected health information, and the app is a means for providing the services.[125]

Similarly, an app developer is a business associate if an app is offered by a health plan, and the app allows users in the network to request, download, and store health plan records and check the status of claims and coverage decisions.[126] The health plan "analyzes the health information and data about app usage to understand effectiveness of its health and wellness offerings."[127] However, the app developer would not be a business associate of the health plan if it offered a direct-to-consumer version of the app that consumers can use to store, manage, and organize their health records and to send health information to providers since the product is not provided on behalf of a covered entity or business associate, as long as the app developer keeps the health information in the two versions of the app completely separate.[128]

III. HIPAA'S APPLICATION TO WEARABLE TECHNOLOGY

Because HIPAA only applies to covered entities and business associates, one of the key questions for wearable technology is who the users of the wearable technology will be and who will have access to the information collected by a device or application.[129] For example, if a consumer inputs his or her own health information into the application and does not share that data with a covered entity or business associate, HIPAA would not apply.[130] Thus, HIPAA does not apply to a Fitbit that simply tracks a user's steps and heart rate, because the information is created by the individual user and not a covered entity or business associate. However, if the device transmits health information to a covered entity (i.e. a physician), the health information could be subject to HIPAA once received by the covered entity, as long as it qualified as protected health information under HIPAA (i.e. individually identifiable information).[131] Therefore, some information on the device may not initially be protected, but could become protected when shared with a physician or other covered entity. For example, if a Fitbit sent a user's activity information to the user's medical record maintained by the user's physician, the activity information could be subject to HIPAA once received by the physician. Another question for wearable technology is who the customers are (i.e. who hired the services or paid for them) and who is directing the

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

129. *See generally* 45 C.F.R. § 160.102 (2015).

130. *See id.*

131. *See generally* 45 C.F.R. § 160.103 (2015).

services. For example, if the covered entity contracts with an app developer or wearable device company to create an app that will transmit health information back to the individual user (i.e. via a messaging option), then that information may be subject to HIPAA as long as it qualified as protected health information.

The illustrations above suggest that companies that manufacture or develop wearable technology or mobile health applications that work with a covered entity or business associate may qualify as a business associate under HIPAA in some situations if they provide services to or perform functions for covered entities or business associates that involve access to protected health information. In these circumstances, the manufacturer or developer may need to meet the HIPAA requirements for business associates, such as maintaining HIPAA policies and procedures, encrypting protected health information in transit and at rest, and conducting risk assessments. They may also be directly liable for certain HIPAA violations and face potential investigation and enforcement action by OCR.[132]

Another issue relevant to wearable technology and mobile health applications concerns data storage. Wearable technology companies may either store health information on their own servers or may contract with a data storage company to store the information.[133] If the data meets the definition of protected health information, and the wearable technology company is a business associate, the data storage company that stores the protected health information on behalf of the wearable technology company could potentially be a business associate of the wearable technology company; thus, a business associate agreement may be needed in some cases. The Omnibus Rule broadened the definition of a business associate to include "[a] subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate,"[134] and the rule's commentary provides some guidance on which entities are considered to be business associates. For example, document storage companies that maintain protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the stored information.[135] In addition, a data storage company that has *access* to protected health information

132. The existence of protected health information alone does not necessarily render a developer of wearable technology or mobile health applications a business associate. Instead, the developer would also need to provide services to or on behalf of a covered entity or business associate that involve the use or disclosure of such protected health information.

133. *See* Nidhi Shah, *Top 11 HIPAA-Compliant Hosting Servers for Healthcare Apps*, ARKENEA (Oct. 5, 2015), http://arkenea.com/blog/top-hipaa-compliant-hosting-servers/.

134. *Id.*

135. 78 Fed. Reg. 5566, 5572 (Jan. 25, 2013).

(whether digital or hard copy) is a business associate, even if the entity does not view the information or only does so on a random or infrequent basis.[136]

Although OCR attempted to provide clarity with this guidance, it has potentially created additional confusion among members of the technology industry. Specifically, the guidance appears to adopt a requirement of "access" not present in the text of the rules. Thus, a question remains as to whether a data storage company that stores encrypted data but does not have access to the encryption key would be considered a business associate.

Additionally, the Omnibus Rule distinguishes between vendors that store protected health information on a transient basis and those that store it on a persistent basis.[137] The "conduit exception" does not consider entities that act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis as business associates.[138] In the Omnibus Rule commentary, HHS stated, "[t]he conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet services providers (ISPs) providing mere data transmission services."[139] As an example, HHS stated that a telecommunications company that has occasional, random access to protected health information when it reviews whether the data transmitted over its network is arriving at its intended destination would not be a business associate.[140] HHS elaborated that "the conduit exception is limited to transmission services (whether digital or hard copy), including any temporary storage of transmitted data incident to such transmission."[141] Thus, an entity that maintains protected health information on behalf of a covered entity would be a business associate and not a mere conduit, even if the entity does not actually view the information.[142] The difference lies in the transient versus the persistent nature of the opportunity to access the protected health information. This analysis may become very important for wearable technology providers in determining whether they or their downstream subcontractors are business associates.

What are some of the best practices for wearable device technology companies and developers to navigate and comply with HIPAA? First, companies developing wearable technology should carefully consider who the users of the device will be and whether protected health information is involved. Involvement of covered entities and business associates in the shar-

136. *Id.* (emphasis added).

137. *Id.*

138. *Id.* at 5571.

139. *Id.*

140. *Id.* at 5571–72.

141. 78 Fed. Reg. at 5572.

142. *Id.*

ing of information will significantly impact whether HIPAA applies, as will the nature of the information at issue and whether it constitutes protected health information.[143] Manufacturers and developers should conduct this HIPAA analysis upfront to ensure that applicable safeguards can be designed and developed as part of the technology they intend to market. For example, HIPAA requires technical safeguards such as encryption (with exceptions in limited circumstances) and the ability to track user log-ins.[144] Compliance with these technical safeguards is even more important now that business associates are directly liable for violations of the Security Rule.[145] Additionally, in certain cases, a wearable device company may need to enter into business associate agreements with its upstream covered entity clients as well as its downstream subcontractors (e.g., a cloud storage company).[146]

Wearable device companies should also carefully consider the structure of their agreements with related parties. While business associates are directly liable for violations of the Security Rule, the major reporting obligations (and related expense) in the event of a breach rest with the covered entity.[147] For example, while the business associate is required to notify the covered entity of a breach, the covered entity is then required to notify HHS, certain individuals, and, potentially, the media.[148] These individual notifications often require significant financial resources such as engaging a public relations firm, establishing a call center, sending individual notice letters, and sometimes providing identity theft protection services.[149] Because the financial burden in the event of a breach by a business associate rests with the covered entity, covered entities often attempt to pass on these financial obligations to their business associates through the use of indemnity provisions in the business associate agreement or other agreements.[150] Thus, the wearable device company will likely want to take a careful look at any indemnification obligations in its business associate agreements with covered entities and may want to include these protections in its agreements with downstream subcontractors.[151]

Finally, wearable device companies must account for the possibility of private civil liability. Although HIPAA does not provide for a private right of

143. *See generally* 45 C.F.R. § 160.103 (2015).

144. *See id.* § 164.312 (2015).

145. *Id.* § 164.306 (2015).

146. *See id.* § 164.502 (2015).

147. *See generally id.* § 164.404 (2015); § 164.406 (2015); § 164.408 (2015).

148. *See, e.g., id.* § 164.404 (2015); § 164.406 (2015); § 164.408 (2015).

149. *See id.* § 164.404 (2015).

150. *See, e.g.*, William Roberts, *Business Associate Agreements – a First Look at Indemnification*, HIPAA.COM, https://www.hipaa.com/business-associate-agreements-a-first-look-at-indemnification/.

151. *See generally id.*

action, courts have recently permitted plaintiffs to pursue state law tort and negligence claims against health care providers and companies for breaches, using HIPAA as the standard of care.[152] Moreover, plaintiffs in data breach litigation more generally have begun to see success in their claims against organizations that have suffered data breaches.[153] We can expect to see more of these lawsuits, and manufacturers and developers should be aware of the risk.

The importance of maintaining HIPAA compliance cannot be overstated for wearable device companies who may be subject to HIPAA. Even if a wearable device company is not required to comply with HIPAA, it may want to comply with certain HIPAA requirements as a best practice to secure health-related information, such as encrypting the information in transit and at rest.[154] The wearable device company should also carefully consider securing comprehensive insurance for data breaches. Another line of protection could include an indemnification provision in an agreement with a developer.[155] Finally, the wearable device company should remain vigilant about potential malware and should regularly update software and implement any necessary security patches.[156] Additional guidance and education from OCR could help manufacturers and developers navigate the complex waters of HIPAA, but so long as they intend to collect and share protected health information from users, they could be subject to OCR's enforcement authority.

IV. FEDERAL TRADE COMMISSION ACT

Even if a device manufacturer or application developer is not subject to HIPAA, it may be subject to the United States Federal Trade Commission's (FTC) enforcement authority.[157] Under the FTC Act, the FTC is charged with preventing companies from engaging in unfair or deceptive acts or practices.[158] The FTC has used this authority to take enforcement action against companies in the healthcare industry that represented to patients and customers that reasonable and appropriate measures to protect their personal information would be taken, but allegedly failed to so.[159]

The FTC regulates data security and the protection of personal information in conjunction with OCR's regulation of protected health information

152. *See, e.g.*, *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014).

153. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

154. *See* 45 C.F.R. § 164.312 (2015).

155. *See generally* Roberts, *supra* note 150.

156. *See generally* 45 C.F.R. § 164.312.

157. 15 U.S.C. §§ 41–58 (2015).

158. *Id.* at § 45.

159. Complaint and Decision and Order, In the Matter of Rite Aid Corp., 150 F.T.C. 694, *2, *5 (2010).

under HIPAA.[160] While the two regulators' authority can overlap, the FTC's authority is broader than OCR's because it is not limited to covered entities and business associates.[161]

Given its broad enforcement power, the FTC can require companies that allegedly violated the law to establish and implement comprehensive privacy programs, conduct risk assessments, designate employees to manage privacy practices, retain independent third parties to periodically assess the company's privacy practices, and provide periodic updates to the FTC regarding privacy practices.[162] In many cases, the obligations outlined in an FTC settlement order have lasted twenty years.[163]

The FTC also has the authority to enforce its own Health Breach Notification Rule.[164] The rule, which the FTC began enforcing in 2010, does not apply to HIPAA covered entities or business associates, but does apply to vendors of personal health records (PHR), PHR related entities, and third-party service providers.[165] As defined in the rule, a PHR includes electronic health information that is identifiable and managed, shared, and controlled by or primarily on behalf of an individual.[166] Companies that are subject to the rule are required to notify affected individuals, the FTC, and, in some cases, the media following a breach of unsecured PHR.[167] Violations of the rule are treated as unfair or deceptive acts or practices under the FTC Act.[168]

In light of the FTC's authority, device manufacturers should take care to craft accurate and straightforward privacy policies, terms of use, or other disclosures regarding the devices' collection, storage, and sharing of personal information.[169] Additionally, manufacturers should take reasonable, industry-

160. U.S. DEP'T OF HEALTH & HUMAN SERVS., OCR Privacy Brief, Summary of the HIPAA Privacy Rule (2003), http://www.helpingyoucare.com/wp-content/uploads/2010/10/Summary-of-the-HIPAA-Privacy-Rule-Office-For-Civil-Rights-Privacy-Brief.pdf.

161. *Id.* at 2–3 (noting OCR's authority extends to covered entities and business associates); 15 U.S.C. § 45(a)(1) (2015) (noting the FTC's authority).

162. *In the Matter of Rite Aid Corp.*, 150 F.T.C. 694, at *5–7.

163. *Id.* at *7.

164. Health Breach Notification Rule, 16 C.F.R. § 318.7 (2016).

165. *Id.* § 318.1(a).

166. *Id.* § 318.2(d).

167. *Id.* § 318.5(b).

168. *Id.* § 318.7.

169. After this article went to print, the Federal Trade Commission (FTC) issued guidance for mobile health app developers. The guidance is available here: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices. The guidance included an interactive tool developed by the FTC in conjunction with other regulators, including HHS and the Food and Drug Administration. It is designed to help app developers identify

standard measures to protect the information their devices collect or share. The FTC's enforcement authority is not limited to conduct involving PHI as that term is defined under HIPAA, but is much broader and could be used to investigate any company that misleads consumers about its privacy practices.

Likewise, manufacturers and application developers should take note of the FTC's Health Breach Notification Rule and take steps to ensure compliance. One simple—but potentially costly—step to avoid application of the rule would be to encrypt any PHR collected. At a minimum, developers should take steps to mitigate the risk of a breach and develop a response plan in the event a breach is suspected.

VI. CONCLUSION

With the use of wearable technology and mobile applications on the rise, there is no doubt these products will multiply and enter new markets. The devices have the potential to help individuals monitor their health and share information with health care providers. But the potential for storing and sharing information also raises legal questions. Companies that enter the fray should think through their products' operation carefully and design those products with federal regulations in mind.

which federal laws and regulations – for example, the FTC ACT, the FTC's Health Breach Notification Rule, HHS's HIPAA, or the FDA's Federal Food, Drug & Cosmetic Act – apply to their apps. *See Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices (last visited May 12, 2016).